RSAC 2025 Conference

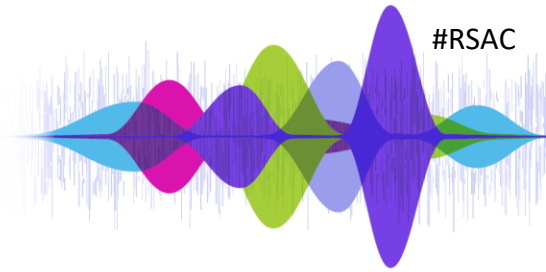
Many Voices.
One Community.

SESSION ID: CRYP-M03A

Quantum Chosen-Ciphertext Attacks Based on Simon's Algorithm against Unified Structures

Xiaoyu Wang

PH.D. Student
Hubei University

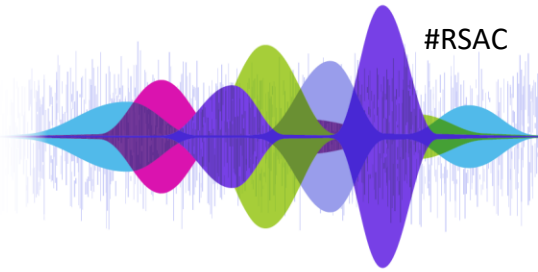


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Outline

- Preliminaries
- Constructing qCCA^d Distinguishers
- Links between qCCA^e Distinguishers and Boomerang Attacks
- Extending qCCA^e Distinguishers
- Applications to Unified Structures
- Conclusion

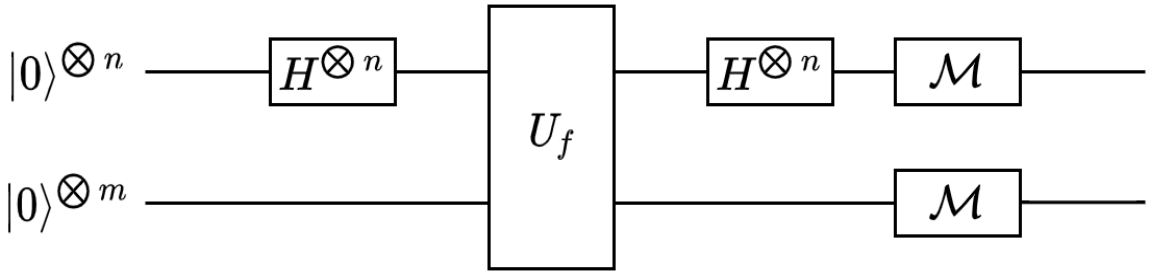
Simon's Algorithm

- Simon's Problem

  $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $f(x) = f(y) \Leftrightarrow x \oplus y \in \{0^n, s\}$, the goal is to find s.

  $f(x) = f(y) \Leftrightarrow y = x \oplus s$ for any distinct x and y is called the Simon's promise.

- Simon's Algorithm



get a random output vector

Orthogonal to s

Solving linear equations (polynomial time complexity)

Exponential acceleration

The Extension of Simon's Algorithm

- A function f satisfying the only condition that $y = x \oplus s \Rightarrow f(x) = f(y)$

[KLL16]

If there exists p_0 such that $\varepsilon(f, s) \leq p_0 < 1$, s can be recovered with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$ after cn queries.

Constructing such distinguishers

[IHM19]

Focusing on the dimension of the vector space spanned by those vectors.

Design periodic functions

[KLL16]. Kaplan, M., Leurent, G., Leverrier, A., & Naya-Plasencia, M. (2016). Breaking symmetric cryptosystems using quantum period finding. In *Advances in Cryptology–CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II 36* (pp. 207-237). Springer Berlin Heidelberg.

[IHM19]. Ito, G., Hosoyamada, A., Matsumoto, R., Sasaki, Y., & Iwata, T. (2019). Quantum chosen-ciphertext attacks against Feistel ciphers. In *Topics in Cryptology–CT-RSA 2019: The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4–8, 2019, Proceedings* (pp. 391-411). Springer International Publishing.

Quantum Distinguisher based on Simon's algorithm

Quantum Distinguishers

- Quantum chosen-plaintext attacks (qCPA) distinguishers
  - only use the encryption oracles
  - must use the decryption oracles
- Quantum chosen-ciphertext attacks (qCCA) distinguishers
  - qCCA^d distinguishers
    - only use decryption oracles
  - qCCA^e distinguishers
    - use the encryption oracles

Quantum distinguishers of several cryptographic structures

Structure	Setting					
	qCPA		qCCA			
			qCCA^d		qCCA^e	
	Round	Ref.	Round	Ref.	Round	Ref.
Feistel	3	[17]	-		4	[14]
Lai-Massey	3	[21]	-		4	[21]
d-Type-1-GFS	3d-3	[23,5]	d^2-d+1	[23,5]	-	
2d-Type-2-GFS	2d+1	[7,5]	2d+1	[5]	-	
d-Type-3-GFS	d+1	[11,30]	-		-	
d-MARS	2d-1	[5]	2d-1	[5]	-	
d-SM4	2d-1	[5,10,4]	2d-1	[5]	-	
d-Skipjack-A	3d-3	[5]	d^2-d+1	[5]	-	
d-Skipjack-B	d^2-d+1	[5]	3d-3	[5]	-	

Constructing qCCA^d Distinguishers

qCCA^e Distinguishers

only using encryption oracles

[XWY24]

General techniques of constructing periodic functions by truncated differentials

qCCA^d Distinguishers

only using decryption oracles

Change the E to E^{-1}

Definition 1 ([XWY24]).

Let $\Delta_O \subset \mathbb{F}_2^n$ be a non-empty set of differences. Assume that there exists a non-zero matrix L and such that $Lx = \gamma$ for any $x \in \Delta_O$, where $\gamma \in \mathbb{F}_2^n$ is a fixed value. Then, we call L a difference-annihilation matrix of Δ_O.

Definition 2 ([XWY24]).

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has an r_2-round truncated differential $\Delta_I \to \Delta_O$ of probability 1, and an r_1-round truncated differential $\delta \to \Delta_I$ of probability 1 with the restriction that one of the inputs belongs to an affine space $w \oplus W$. If there exists a difference-annihilation matrix M of Δ_O , and the projection of δ to $W^{\perp}$ is known, then we can define a periodic function $g: \mathbb{F}_2 \times \mathbb{F}_2^t \to \mathbb{F}_2^k,\ (b, x) \mapsto M \cdot E_{r_1+r_2}\left(w_b \oplus \varphi(x)\right) \oplus \gamma_b$, where $\varphi: \mathbb{F}_2^t \to W$ be a bijective linear transformation, $w_0 = w, w_1 = w \oplus \delta^{\perp}$, and γ_0, γ_1 be two constants such that $\gamma_0 \oplus \gamma_1 = \gamma$. Moreover, we call such a periodic function a Type-II periodic function of $E_{r_1+r_2}$, where $E_{r_1+r_2}$ is the $(r_1 + r_2)$-round reduced version of E.

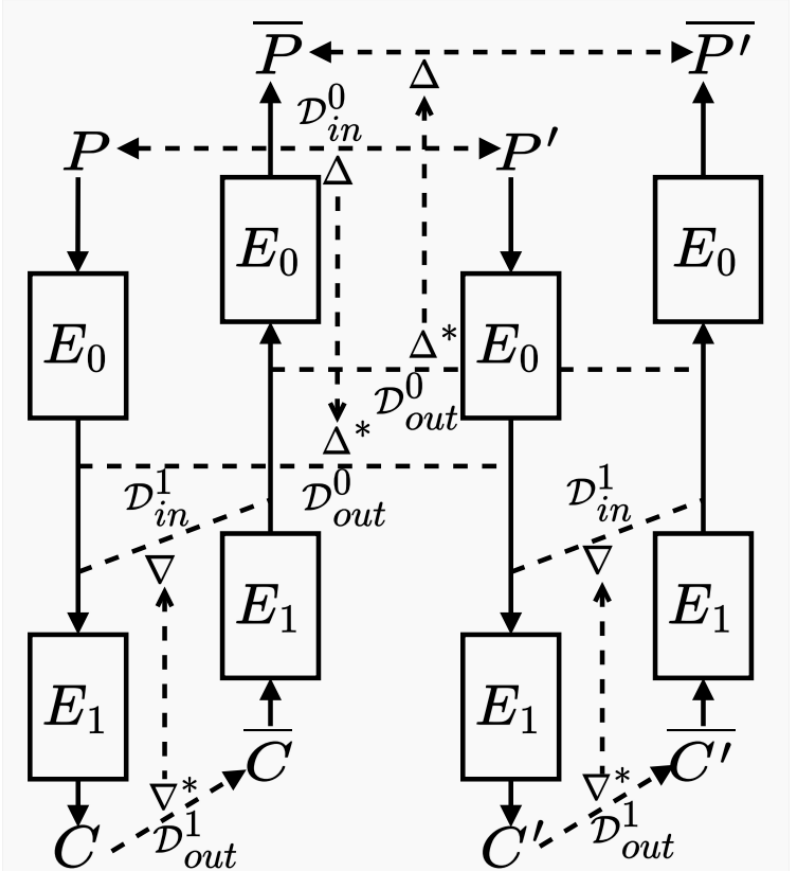
E → E^{-1} qCCA^d distinguishers

The periodic functions used in qCCA^d distinguishers of Type-1 GFS, Type-2 GFS, SM4-like, MARS-like and Skipjack-A/B are also Type-II periodic functions.

[XWY24] Xiang, Z., Wang, X., Yu, B., Sun, B., Zhang, S., Zeng, X., Shen, X., Li, N. Links between quantum distinguishers based on Simon's algorithm and truncated differentials. *IACR Transactions on Symmetric Cryptology*.

Truncated Boomerang Distinguishers

- Choose a random plaintext pair (P, P') with $P \oplus P' \in \mathcal{D}_{in}^{0}$, query the corresponding ciphertext pair (C, C').
- Shift the ciphertext pair (C, C') into new pair $(\overline{C}, \overline{C'})$, such that $C \oplus \overline{C}, C' \oplus \overline{C'} \in \mathcal{D}_{out}^{1}$, query the decryption of $(\overline{C}, \overline{C'})$ to $(\overline{P}, \overline{P'})$.
- If $\overline{P} \oplus \overline{P'} \in \mathcal{D}_{in}^{0}$ holds, then $(P, P', \overline{P}, \overline{P'})$ is the truncated boomerang quartet.
- Then the attacker can use the difference in the probability that $(P, P', \overline{P}, \overline{P'})$ is a truncated boomerang quartet to accomplish the truncated boomerang distinguishing attack.

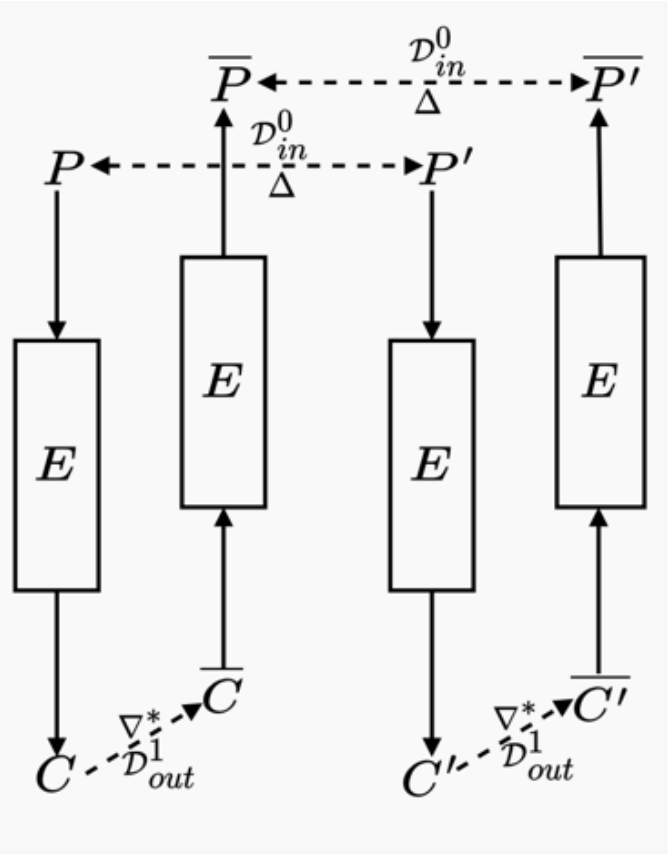


Observations on Boomerang Attacks

Definition 3.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher. We define the probability of the boomerang differential (Δ, ∇^*) for E as

$$\Pr[\, E^{-1}(E(P) \oplus \nabla^*) \oplus E^{-1}(E(P') \oplus \nabla^*) = \Delta \mid P \oplus P' = \Delta \,].$$



Definition 4.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, $\mathcal{D}_{in}^0, \mathcal{D}_{out}^1$ be two subsets of $\mathbb{F}_2^n$. We define the probability of the truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1)$ for E as

$$\Pr\left[\, E^{-1}\left(\overline{C}\right) \oplus E^{-1}\left(\overline{C'}\right) \in \mathcal{D}_{in}^0 \mid P \oplus P' \in \mathcal{D}_{in}^0, E(P) \oplus \overline{C}, E(P') \oplus \overline{C'} \in \mathcal{D}_{out}^1 \,\right].$$

Periodic Functions and Truncated Boomerang Differentials

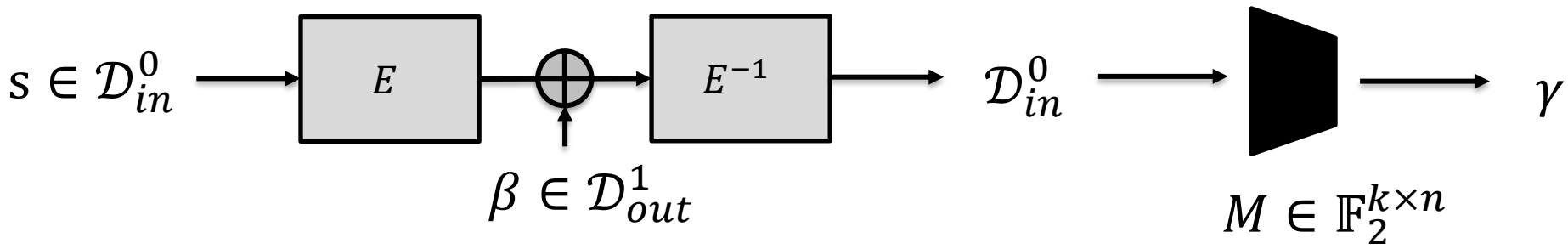
Theorem 1.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has a probability 1 truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1)$. Assume that there exists a difference-annihilation matrix $M \in \mathbb{F}_2^{k \times n}$ of row full rank, such that $Mx = \gamma$ is a fixed constant for any $x \in \mathcal{D}_{in}^0$. Let γ_0 and γ_1 be two k-bit constants, such that $\gamma_0 \oplus \gamma_1 = \gamma$. Then, for any $\beta \in \mathcal{D}_{out}^1$ with $\beta \neq 0^n$, we can define a function g as

$$g: \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^k$$

$$(b, x) \mapsto M \cdot E^{-1}(E(x) \oplus \beta) \oplus \gamma_b.$$

Then, g is a periodic function, $(1, s)$ is a period of g for any $s \in \mathcal{D}_{in}^0$.



Periodic Functions and Boomerang Differentials

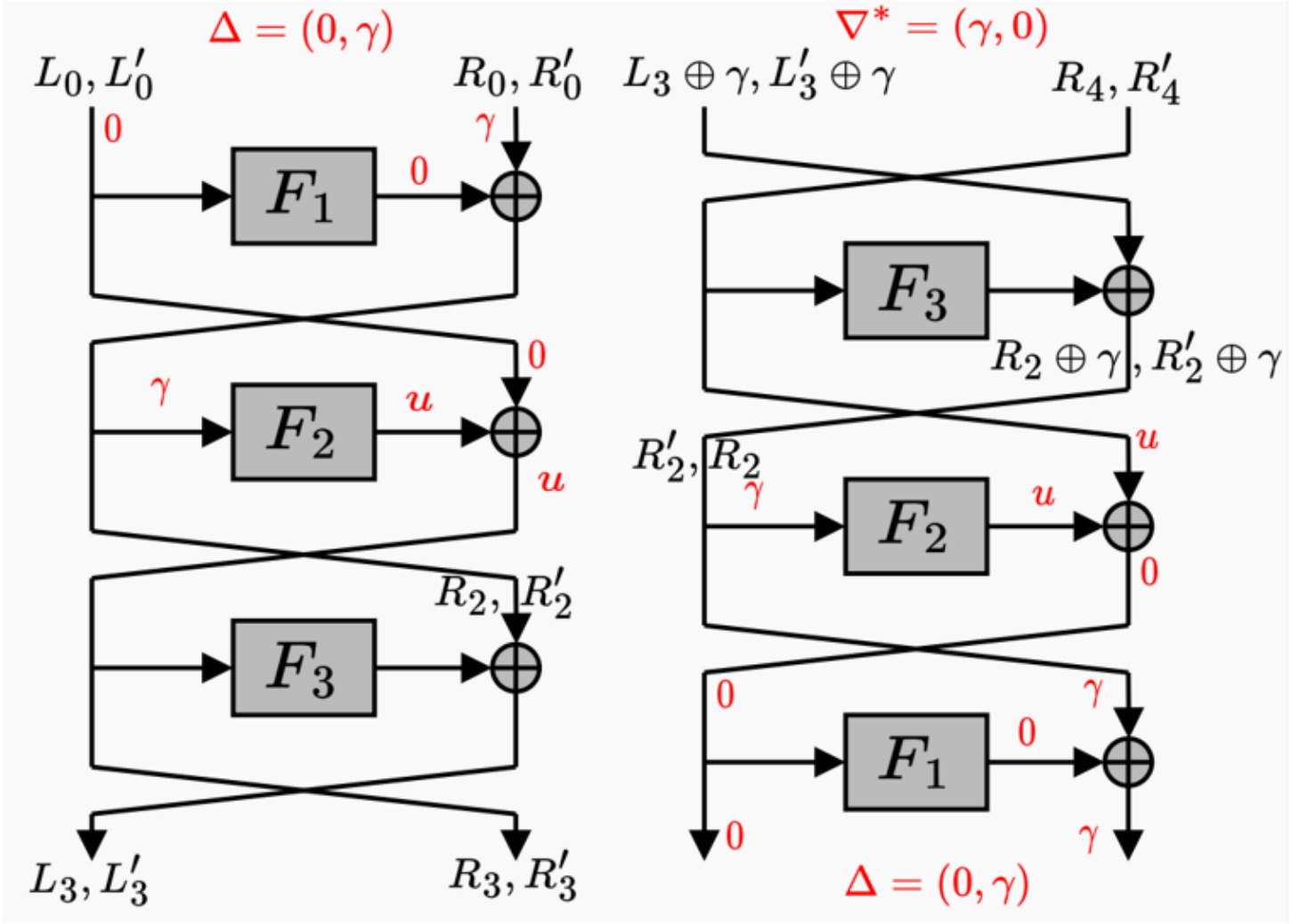
Corollary 1.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has a probability 1 boomerang differential (Δ, ∇^*). Let Δ_0 and Δ_1 be two k-bit constants, such that $\Delta_0 \oplus \Delta_1 = \Delta$. Define a function g as

$$g: \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^k$$
$$(b, x) \mapsto E^{-1}(E(x) \oplus \nabla^*) \oplus \Delta_b.$$

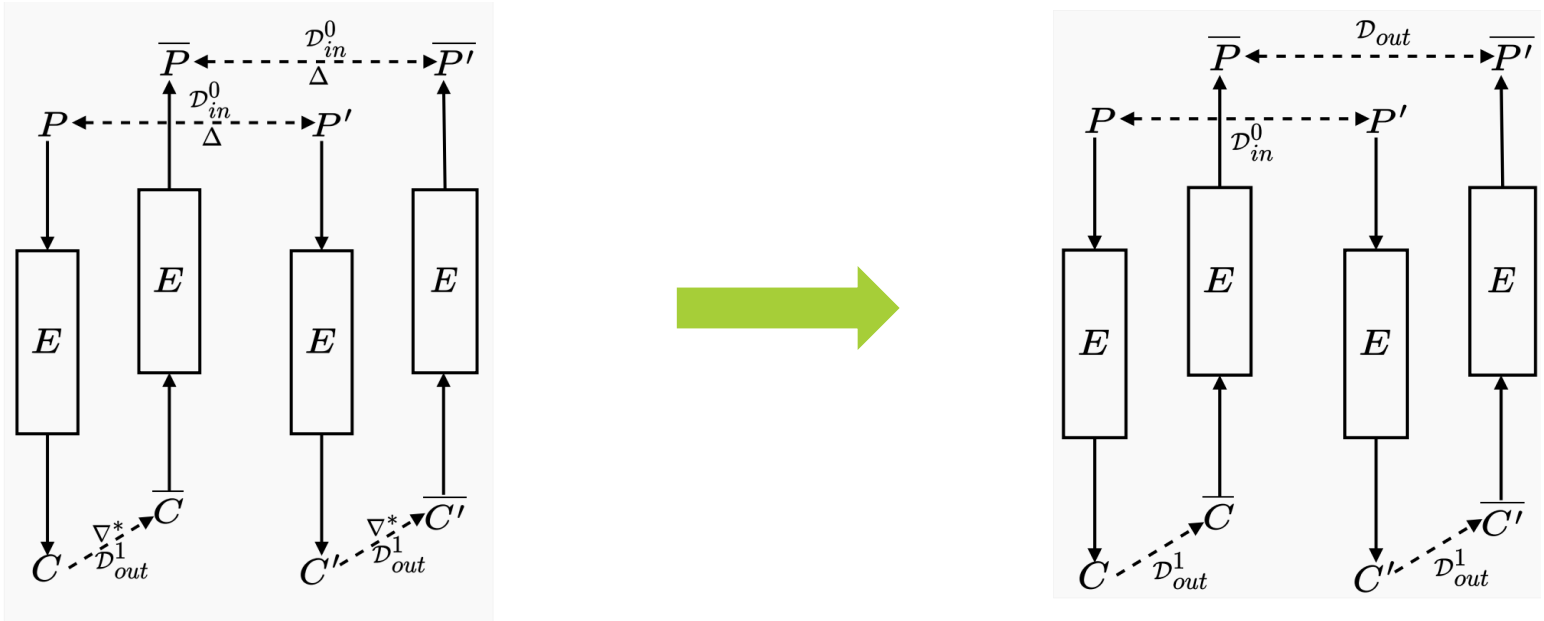
Then, g is a periodic function with $(1, \Delta)$ being its period.

Example 1 —3-Round Feistel Structure



$$g_1(b, y, z) = \mathcal{E}_3^{\text{Feistel},-1}[\mathcal{E}_3^{\text{Feistel}}(y, z) \oplus \nabla^*] \oplus (0, \gamma_b)$$

Improved Truncated Boomerang Differentials



Definition 5.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, $\mathcal{D}_{in}^0, \mathcal{D}_{out}^1$ and $\mathcal{D}_{out}$ be three subsets of $\mathbb{F}_2^n$. We define the probability of the improved truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1, \mathcal{D}_{out})$ for E as

$$\Pr\left[E^{-1}(\overline{C}) \oplus E^{-1}(\overline{C'}) \in \mathcal{D}_{out} \mid P \oplus P' \in \mathcal{D}_{in}^0, E(P) \oplus \overline{C}, E(P') \oplus \overline{C'} \in \mathcal{D}_{out}^1 \right].$$

Periodic Functions and Improved Truncated Boomerang

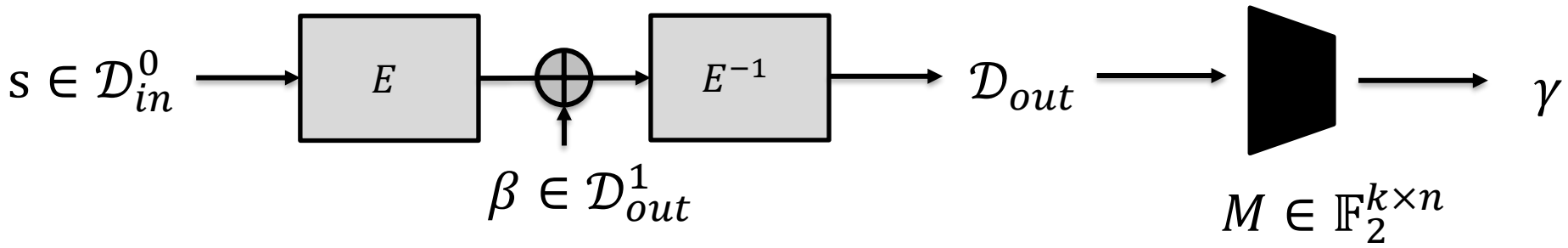
Theorem 2.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which has an improved truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1, \mathcal{D}_{out})$ with probability 1. Assume that there exists a difference-annihilation matrix $M \in \mathbb{F}_2^{k\times n}$ of row full rank, such that $Mx = \gamma$ is a fixed constant for any $x \in \mathcal{D}_{out}$. Let γ_0 and γ_1 be two k-bit constants, such that $\gamma_0 \oplus \gamma_1 = \gamma$. Then, for any $\beta \in \mathcal{D}_{out}^1$ with $\beta \neq 0^n$, we can define a function g as

$$g: \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^k$$

$$(b, x) \mapsto M \cdot E^{-1}(E(x) \oplus \beta) \oplus \gamma_b.$$

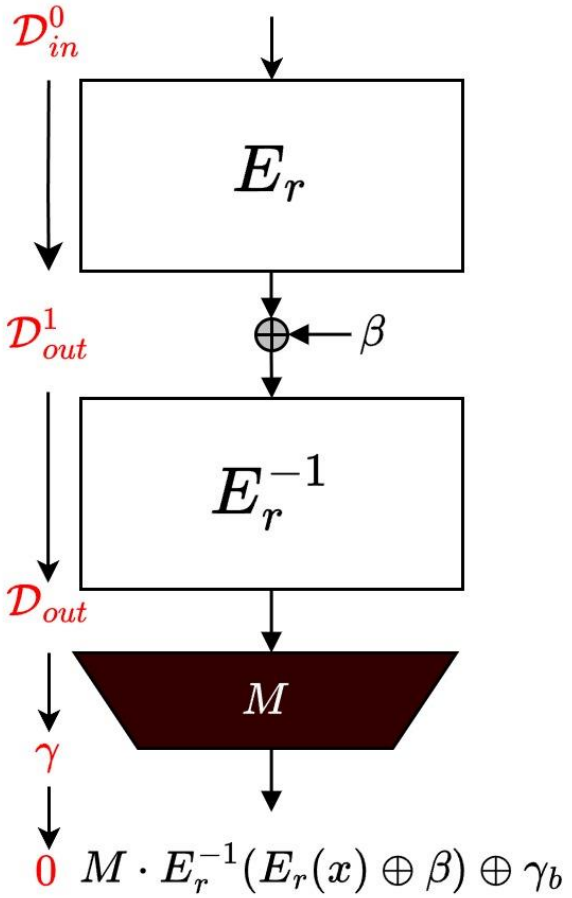
Then, g is a periodic function, and $(1, s)$ is a period of g for any $s \in \mathcal{D}_{in}^0$.



Type-III Periodic Functions

Definition 6.

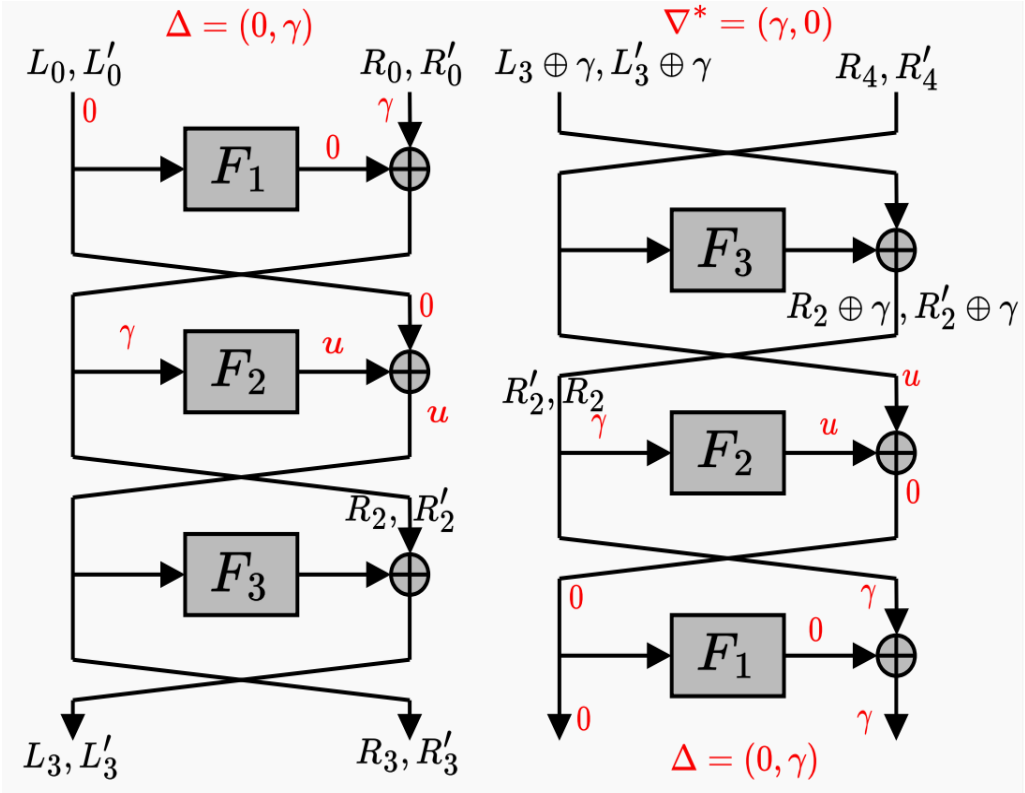
Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which satisfies that E_r has an improved truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1, \mathcal{D}_{out})$ with probability 1. If there exists a difference-annihilation matrix of $\mathcal{D}_{out}$, we call the periodic function as constructed in Theorem 1 a Type-III periodic function of E_r, where E_r is the r-round reduced version of E.



Quantum Distinguishers of Feistel Structures

3-Round Distinguisher

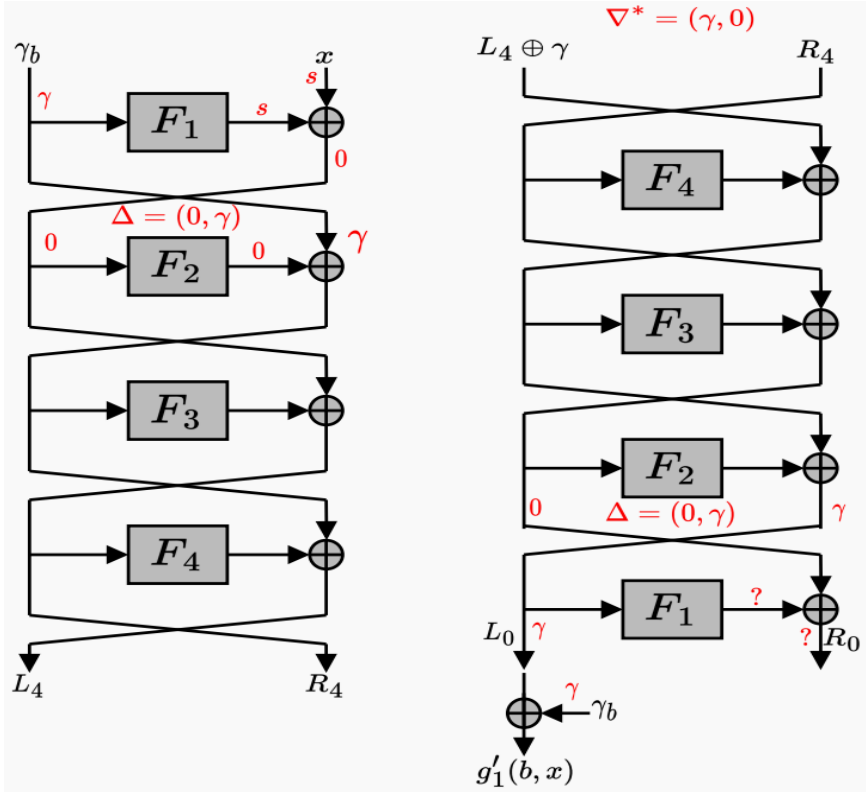
Type-III periodic function



$$g_1(b, y, z) = \mathcal{E}_3^{\text{Feistel},-1}[\mathcal{E}_3^{\text{Feistel}}(y, z) \oplus \nabla^*] \oplus (0, \gamma_b)$$

4-Round Distinguisher

[IHM19]



$$g_1'(b, x) = L_0 \oplus \gamma_b$$

$$(L_0, R_0) = \mathcal{E}_4^{\text{Feistel},-1}(L_0 \oplus \gamma, R_4) \quad (L_4, R_4) = \mathcal{E}_4^{\text{Feistel}}(\gamma_b, x)$$

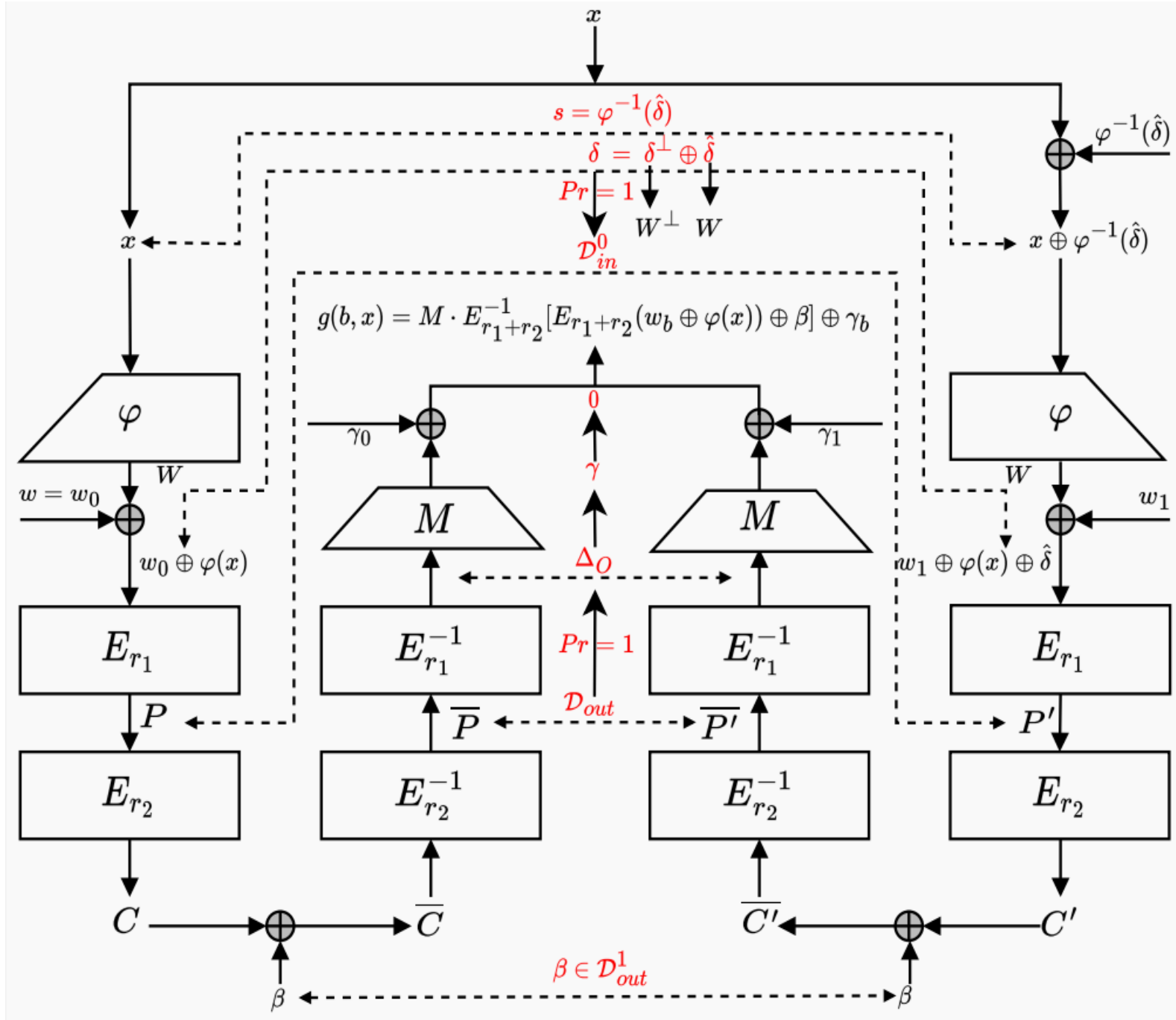
Extending qCCA^e Distinguishers

Theorem 3.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which satisfies that E_{r_2} has an improved truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1, \mathcal{D}_{out})$ with probability 1. Assume that there exists a probability 1 truncated differential $\mathcal{D}_{out} \to \Delta_O$ for $E_{r_1}^{-1}$, and a difference-annihilation matrix $M \in \mathbb{F}_2^{k \times n}$ of row full rank, such that $Mx = \gamma$ is a fixed constant for any $x \in \mathcal{D}_{out}$. Moreover, assume that E has a r_1-round difference transition $\delta \to \mathcal{D}_{in}^0$ with probability of 1 when one of the inputs belongs to a t-dimensional $(t < n)$ affine space $w \oplus W$, where $W = \text{span}\{\zeta_1, \zeta_2, \ldots, \zeta_t\}$, (i.e., $\zeta_1, \zeta_2, \ldots, \zeta_t$ constitute a basis of W). Denote $\delta^{\perp}$ the projection of δ to $W^{\perp}$, and $\hat{\delta}$ the projection of δ to W. Let φ be a bijective linear transformation, and φ is defined as $\varphi: \mathbb{F}_2 \times \mathbb{F}_2^t \to W$, $(x_1, \ldots, x_t) \mapsto x_1\zeta_1 \oplus \cdots \oplus x_t\zeta_t$. Let $w_0 = w$, $w_1 = w \oplus \delta^{\perp}$, and γ_0, γ_1 be two constants such that $\gamma = \gamma_0 \oplus \gamma_1$. Then, for any $\beta \in \mathcal{D}_{out}^1$ with $\beta \neq 0^n$, we can define a function g as

$$g: \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^k$$
$$(b, x) \mapsto M \cdot E_{r_1+r_2}^{-1}\left(E_{r_1+r_2}(\mathrm{w}_b \oplus \varphi(x)) \oplus \beta\right) \oplus \gamma_b.$$

Then, g is a periodic function with a period $(1, s)$, where $s = \varphi^{-1}(\hat{\delta})$.


x
$s = \varphi^{-1}(\hat{\delta})$
$\delta = \delta^{\perp} \oplus \hat{\delta}$
$Pr = 1$
$W^{\perp}$
W
$\mathcal{D}_{in}^{0}$
$\varphi^{-1}(\hat{\delta})$
$x \oplus \varphi^{-1}(\hat{\delta})$
$g(b, x) = M \cdot E_{r_1+r_2}^{-1}[E_{r_1+r_2}(w_b \oplus \varphi(x)) \oplus \beta] \oplus \gamma_b$
φ
W
$w = w_0$
$w_0 \oplus \varphi(x)$
E_{r_1}
P
E_{r_2}
C
β
γ_0
0
γ
M
Δ_O
$E_{r_1}^{-1}$
$Pr = 1$
$\mathcal{D}_{out}$
$\overline{P}$
$E_{r_2}^{-1}$
$\overline{C}$
γ_1
M
$E_{r_1}^{-1}$
$\overline{P'}$
$E_{r_2}^{-1}$
$\overline{C'}$
$\beta \in \mathcal{D}_{out}^{1}$
β
φ
W
w_1
$w_1 \oplus \varphi(x) \oplus \hat{\delta}$
E_{r_1}
P'
E_{r_2}
C'

Type-IV Periodic Functions

Definition 7.

Let $E: \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a block cipher, which satisfies that E_{r_2} has an improved truncated boomerang differential $(\mathcal{D}_{in}^0, \mathcal{D}_{out}^1, \mathcal{D}_{out})$ with probability 1. Moreover, E_{r_1} has a probability 1 truncated differential $\delta \to \mathcal{D}_{in}^0$ with the restriction that one of the inputs belongs to an affine space $w \bigoplus W$ and $E_{r_1}^{-1}$ has a probability 1 truncated differential $\mathcal{D}_{out} \to \Delta_O$. If there exists a difference-annihilation matrix M of Δ_O and the projection of δ to $W^{\perp}$ is known, then we call the periodic function as constructed in Theorem a Type-IV periodic of $E_{r_1+r_2}$.

Remark 1.

Interchanging E and E^{-1} in Theorem (Theorem), the corresponding periodic functions still can be constructed. The method remains essentially unchanged, so the periodic function obtained by interchanging E and E^{-1} in Definition 1 (Definition 2) is also called a Type-III (Type-IV) periodic function.

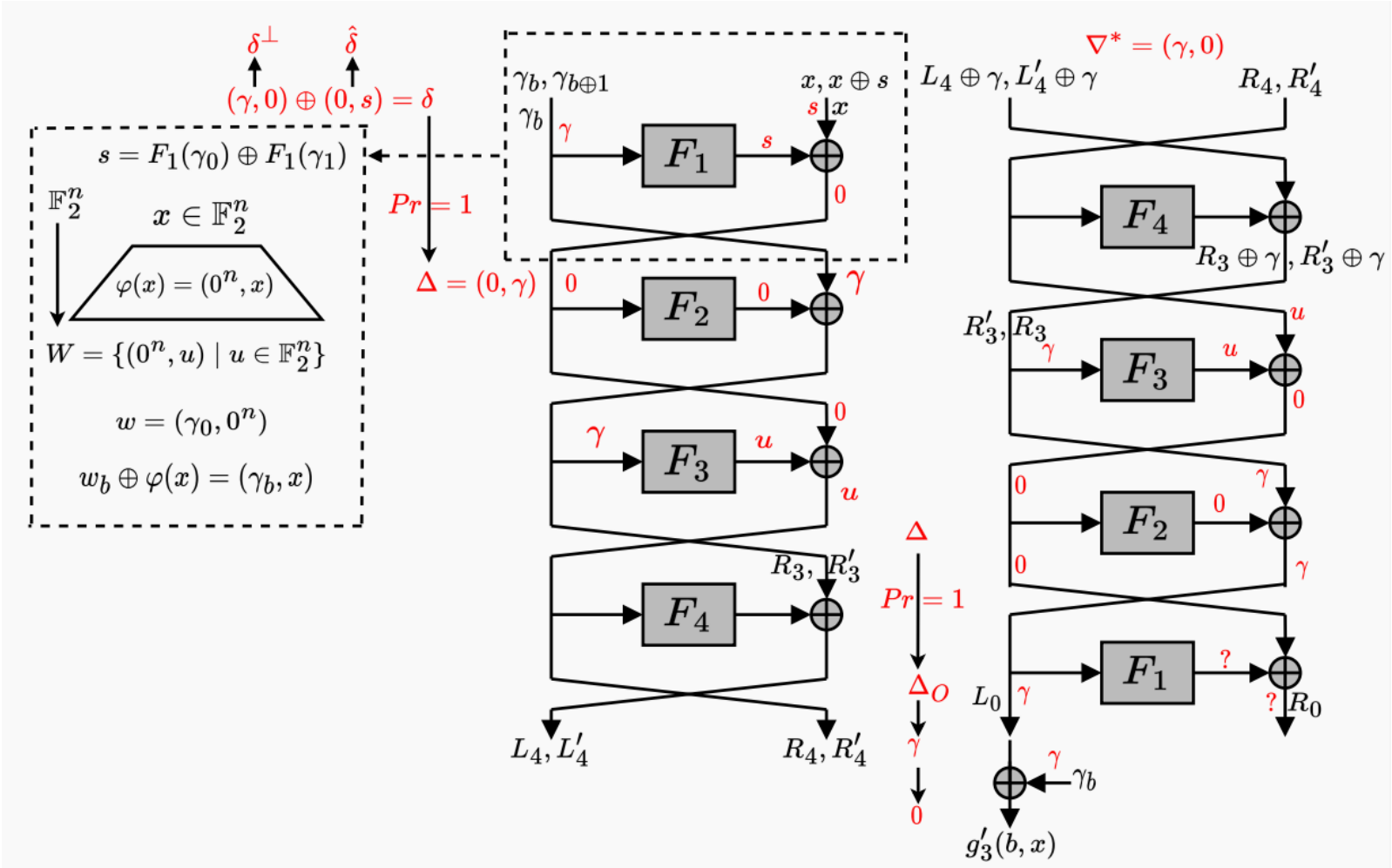
Example 2 — 4-Round Feistel Structure

- Ito *et al.* work [IHM+19]

$$g_1'(b,x) = L_0 \oplus \gamma_b$$

$$(L_0, R_0) = \mathcal{E}_4^{\text{Feistel},-1}(L_4 \oplus \gamma, R_4)$$

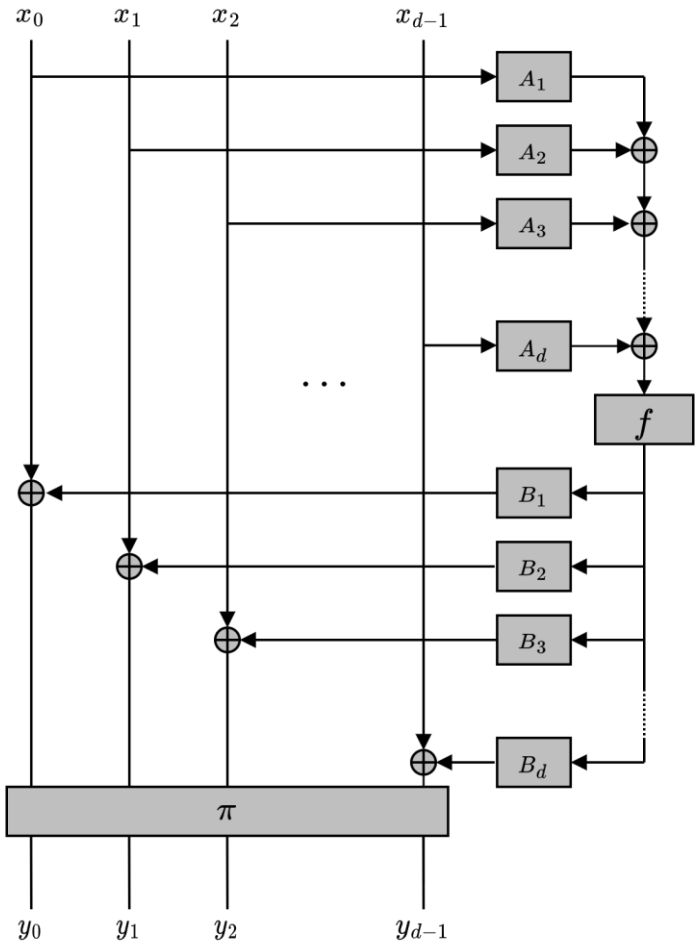
$$(L_4, R_4) = \mathcal{E}_4^{\text{Feistel}}(\gamma_b, x)$$



- Type-IV periodic function

$$g_1'(b,x) = M_1 \cdot \mathcal{E}_4^{\text{Feistel},-1}\left[\mathcal{E}_4^{Feistel}(\gamma_b, x) \oplus \nabla^*\right] \oplus \gamma_b \qquad M_1 = (O\ I)$$

Unified Structure

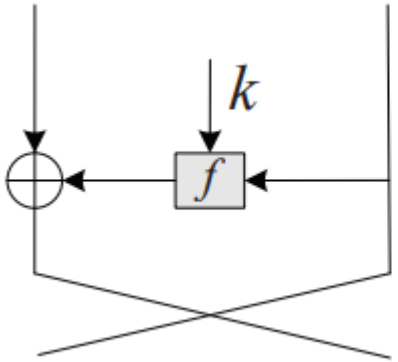


[LSL22]

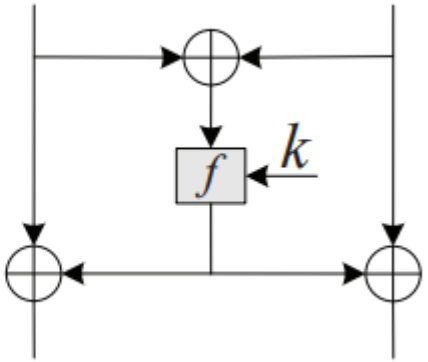
- $A = (A_1 \dots A_d)\ B = \left(B_1^{\mathrm{T}} \dots B_d^{\mathrm{T}}\right)^{\mathrm{T}}$
- r-round unified structure $\mathcal{F}_{A,B,\pi}(f_1, \dots, f_r)$, f_i is the i-the round function
- $\mathcal{A}^r = \begin{pmatrix} A \\ A\pi \\ \vdots \\ A\pi^r \end{pmatrix}$ $\mathcal{B}^r = (B\ \pi B\ \cdots\ \pi^r B)$

[LSL22]. Liu, J., Sun, B., Liu, G., Dong, X., Liu, L., Zhang, H., & Li, C. (2022). New Wine Old Bottles: Feistel Structure Revised. *IEEE Transactions on Information Theory*.

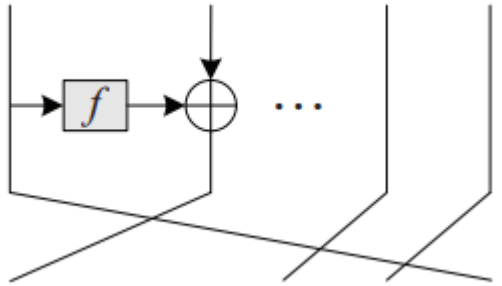
Special Instances of the Unified Structure



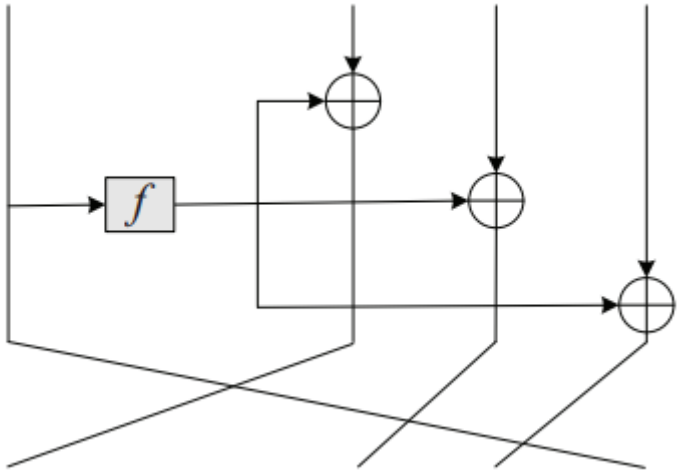
Feistel



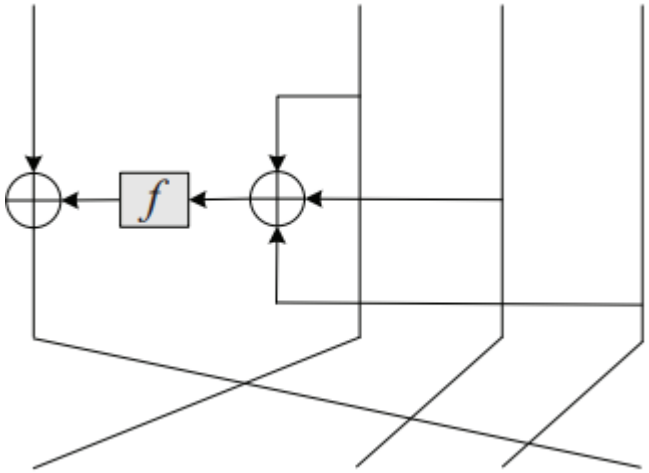
Lai-Massey



Type-1 generalized Feistel

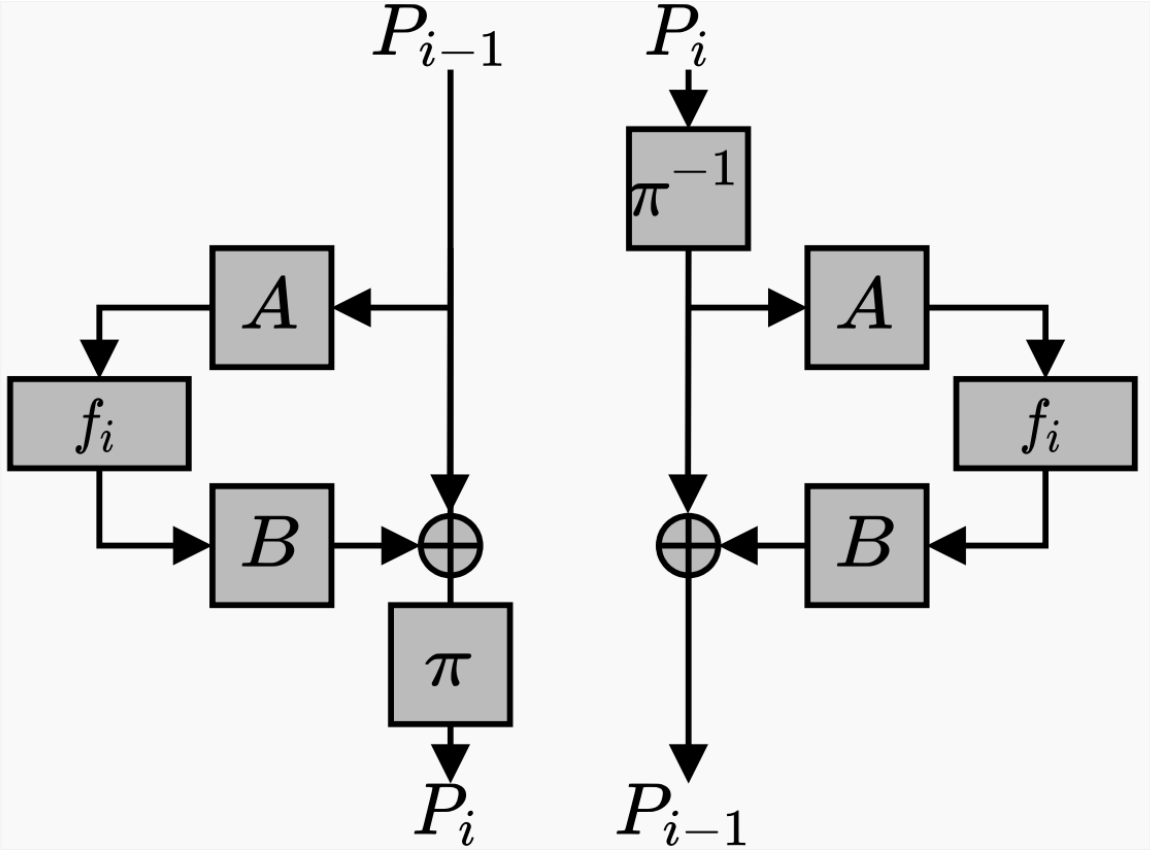


SM4



MARS

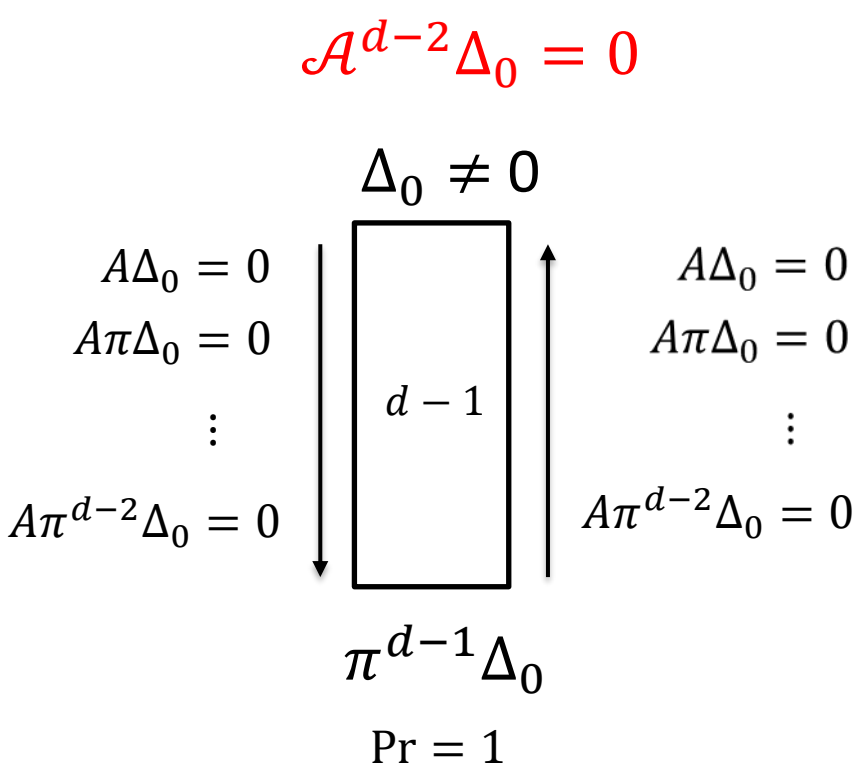
Inverse of Unified Structure

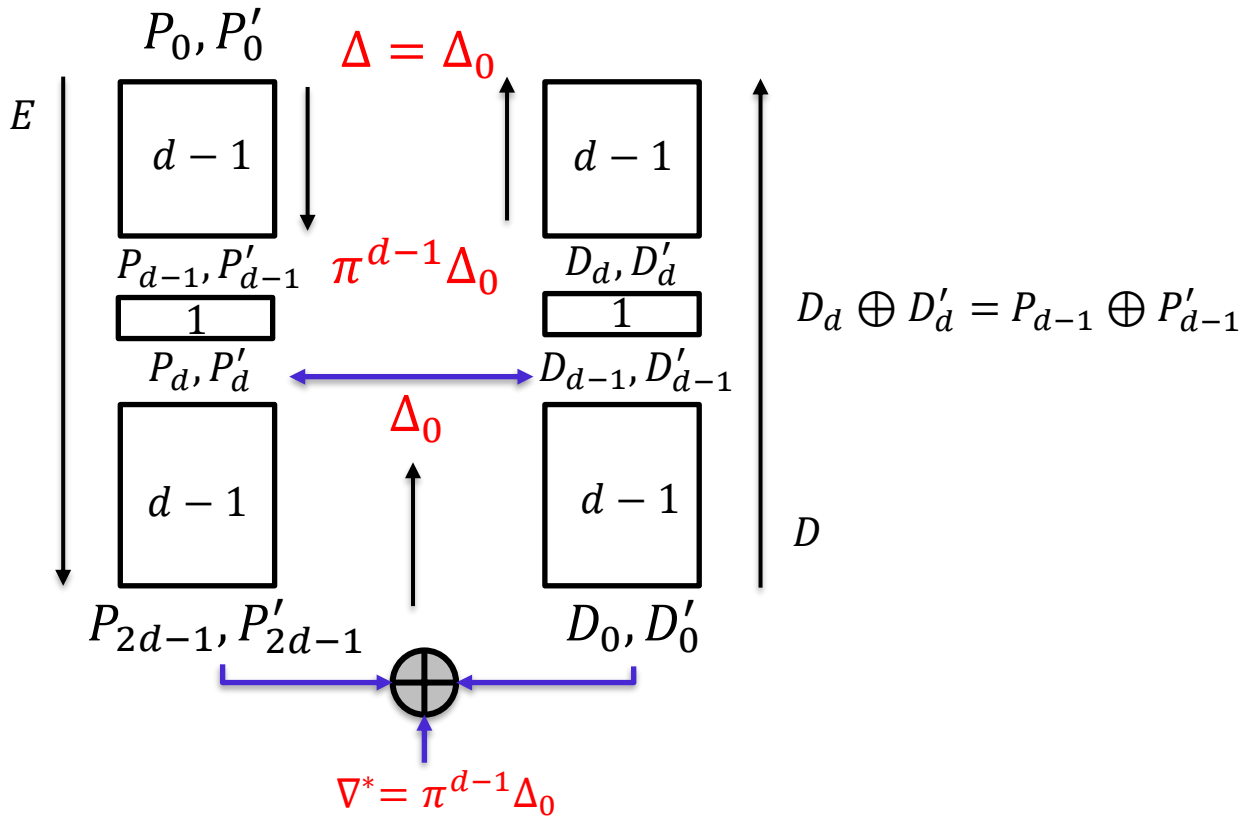


- $A = (A_1 \dots A_d)$
- $B = \left(B_1^{\mathrm{T}} \dots B_d^{\mathrm{T}}\right)^{\mathrm{T}}$
- $AB = \sum_{i=1}^{d} A_i B_i = O$
- $\mathcal{F}_{A,B,\pi}^{-1}(f_1, \dots, f_r)$

Proposition 1.

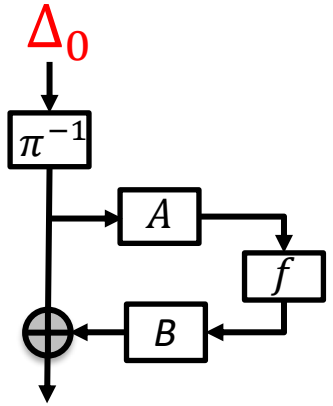
Let $\mathcal{F}_{A,B,\pi}(f_1,\ldots,f_{2d-1})$ be a unified structure with d branches and each of size n bits, where $A \in \mathbb{F}_2^{m\times nd}$, $B \in \mathbb{F}_2^{nd\times m}$. Moreover $\mathrm{AB} = O$, $\mathrm{rank}(\mathcal{A}^{d-2}) < \mathrm{nd}$. Then, there always exists boomerang differential (Δ, ∇^*) with probability 1 for $\mathcal{F}_{A,B,\pi}(f_1,\ldots,f_{2d-1})$.





Proposition 2.

Let $\mathcal{F}_{A,B,\pi}(f_1,\ldots,f_{2d})$ be a unified structure with d branches and each of size n bits, where $A \in \mathbb{F}_2^{m\times nd}$, $B \in \mathbb{F}_2^{nd\times m}$. Moreover $\mathrm{AB} = O$, $\mathrm{rank}(\mathcal{A}^{d-2}) < nd$ and $\mathrm{rank}(B) < nd$. Then, there always exists a Type-IV periodic function for $\mathcal{F}_{A,B,\pi}(f_1,\ldots,f_{2d})$.



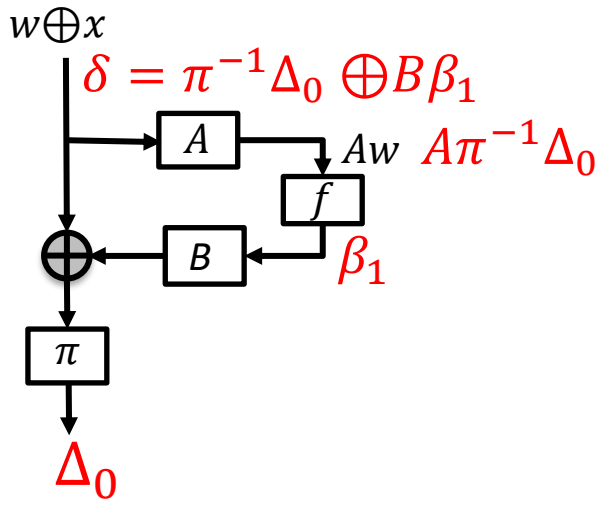
$$\Pr[\{\Delta_0\} \rightarrow \{\pi^{-1}\Delta_0 \oplus Bu \mid u \in \mathbb{F}_2^m\}] = 1$$

$$\mathrm{rank}(B) < nd \longrightarrow \exists M, MB = O$$

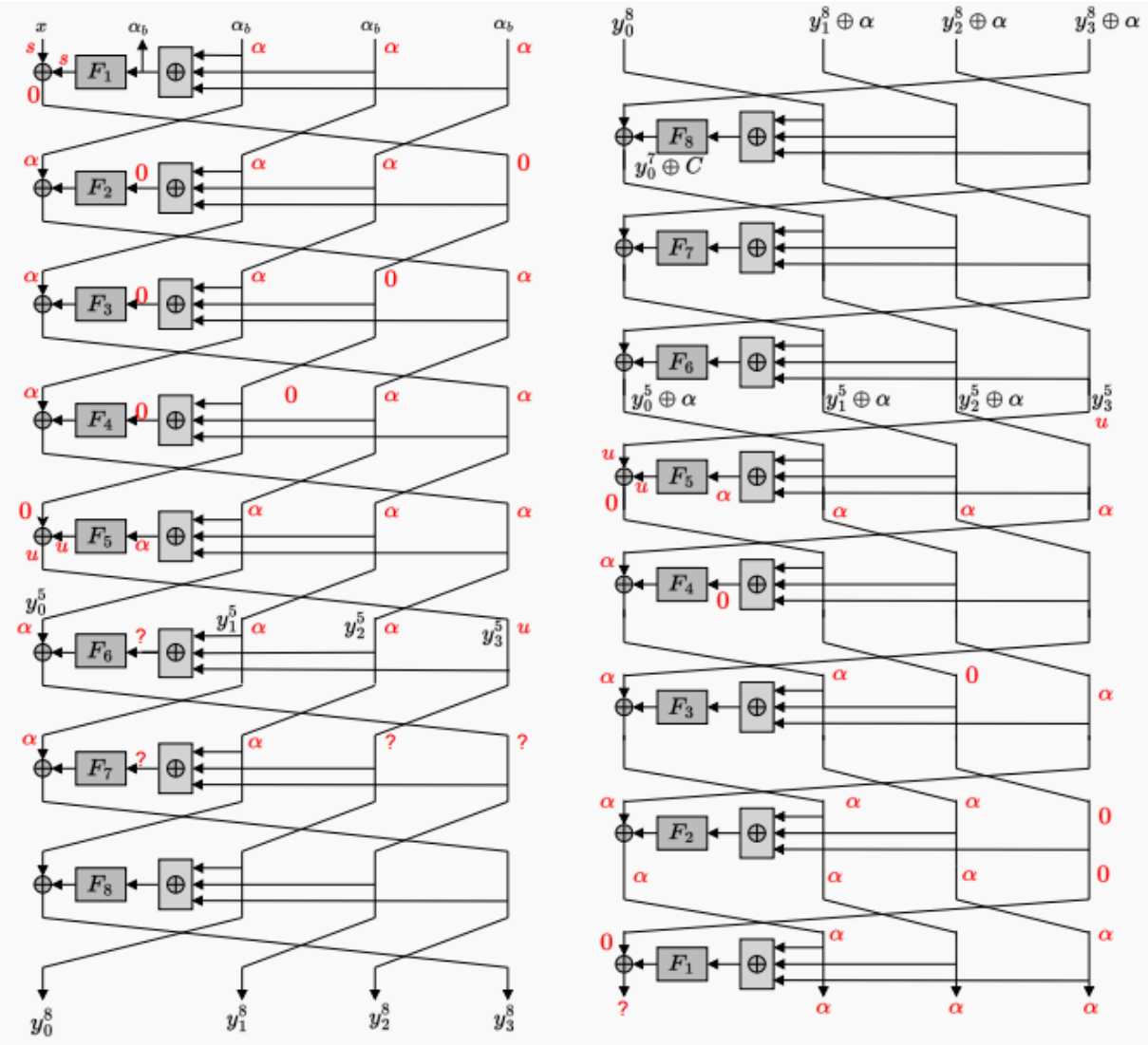
$$M(\pi^{-1}\Delta_0 \oplus Bu) = M\pi^{-1}\Delta_0$$

$$W = \{x \in \mathbb{F}_2^{nd} \mid Ax = 0\}$$

$$w \in W^{\perp} \quad AB = O$$



8-Round Distinguisher of SM4



$$A = (O\ I\ I\ I)\ B = (I\ O\ O\ O)^{\mathrm{T}}$$

$$\mathcal{A}^2 = \begin{pmatrix} A \\ A\pi \\ A\pi^2 \end{pmatrix} = \begin{pmatrix} O & I & I & I \\ I & O & I & I \\ I & I & O & I \end{pmatrix}$$

$$\mathcal{A}^2(\alpha, \alpha, \alpha, 0) = 0$$

$$\Delta = \Delta_0 = (\alpha, \alpha, \alpha, 0)$$

$$\nabla^* = \pi^{-1}\Delta_0 = \pi^3\Delta_0 = (0, \alpha, \alpha, \alpha)$$

$$M_2 = (O\ I\ I\ I) \qquad M_2 B = O$$

$$W = \{(x, 0,0,0) \mid x \in \mathbb{F}_2^{32}\}$$

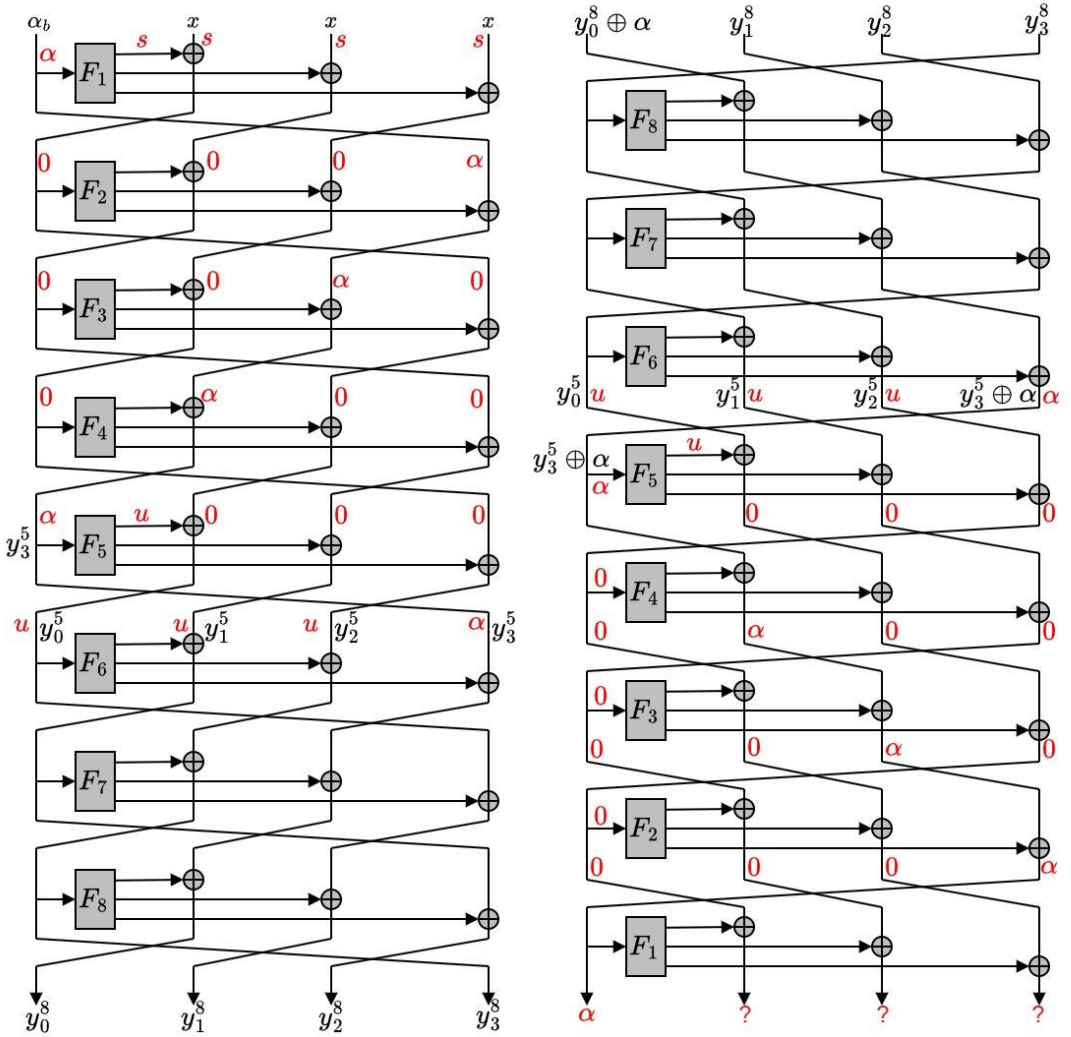
$$\delta = \pi^{-1}\Delta_0 \oplus B\beta_1 = (s, \alpha, \alpha, \alpha) \rightarrow \Delta_0$$

$$\beta_1 = F_1(\alpha_0) \oplus F_1(\alpha_1) = s$$

$$g_2 : \mathbb{F}_2 \times \mathbb{F}_2^{32} \rightarrow \mathbb{F}_2^{32}$$

$$(b, x) \mapsto M_2 \cdot \mathcal{E}_8^{\mathrm{SM4},-1}\left[\mathcal{E}_8^{\mathrm{SM4}}\ (x, \alpha_b, \alpha_b\alpha_b) \oplus (0, \alpha, \alpha, \alpha)\right] \oplus \alpha_b$$

8-Round Distinguisher of MARS



$$A = (I\ O\ O\ O)\quad B = (O\ I\ I\ I)^{\mathrm{T}}$$

$$\mathcal{A}^2 = \begin{pmatrix} A \\ A\pi \\ A\pi^2 \end{pmatrix} = \begin{pmatrix} I & O & O & O \\ O & I & O & O \\ O & O & I & O \end{pmatrix}$$

$$\mathcal{A}^2(0,0,0,\alpha) = 0$$

$$\Delta = \Delta_0 = (0,0,0,\alpha)$$

$$\nabla^* = \pi^{-1}\Delta_0 = \pi^3\Delta_0 = (\alpha,0,0,0)$$

$$M_3 = (I\ O\ O\ O)\quad M_3 B = O$$

$$W = \{(0,x,x,x) \mid x \in \mathbb{F}_2^{32}\}$$

$$\delta = \pi^{-1}\Delta_0 \oplus B\beta_1 = (\alpha,s,s,s) \to \Delta_0$$

$$\beta_1 = F_1(\alpha_0) \oplus F_1(\alpha_1) = s$$

$$g_3 : \mathbb{F}_2 \times \mathbb{F}_2^{32} \to \mathbb{F}_2^{32}$$

$$(b,x) \mapsto M_3 \cdot \mathcal{E}_8^{\mathrm{MARS},-1}\left[\mathcal{E}_8^{\mathrm{MARS}}(\alpha_b,x,x,x) \oplus (\alpha,0,0,0)\right] \oplus \alpha_b$$

Conclusion

- Constructing qCCA^d distinguishers
  - Transform to construct qCCA^e distinguishers
  - General techniques of constructing periodic functions with truncated differentials
- Constructing qCCA^e distinguishers
  - Links between qCCA^e distinguishers and boomerang differentials
  - Define two types of periodic functions: Type-III/IV
  - General approaches to constructing qCCA^e distinguishers exploiting improved truncated boomerang differential with probability 1
- Applications to Unified Structures
  - Prove the existence of $(2d-1)$-round boomerang differential
  - Extend one round, $2d$-round , covering Feistel, Lai-Massey, SM4-like, MARS-like structures
    - SM4/MARS-like, the best previous results：$2d-1$
    - 8-round MARS is SPRP, not a qPRP in chosen-ciphertext settings

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank you!

RSAC 2025 Conference

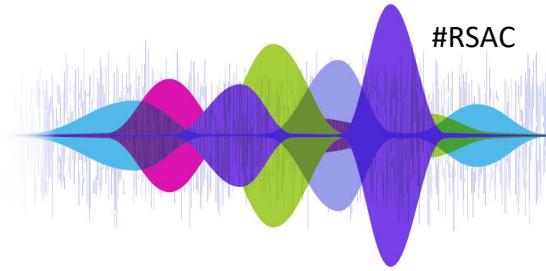
Many Voices.
One Community.

SESSION ID: CRYP-M03B

Improved Key Recovery Attacks of Ascon

Shuo Peng, Kai Hu, Jiahui He, Meiqin Wang

School of Cyber Science and Technology, Shandong University

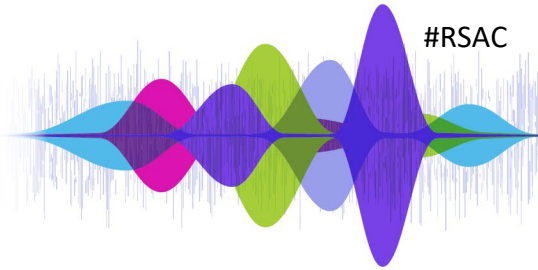


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Outline

- Introduction
- The Ascon AEAD
- Key recovery in the misuse-free setting
- Key recovery in the misused setting
- Conclusion

RSAC 2025 Conference

Introduction

Motivation

- Ascon is a family of lightweight AEAD mode and hash functions
- Winner of the CAESAR competition(lightweight category)
- Standardized by NIST in 2023
- Attacks of Ascon-128
  - No attacks poses a threat beyond the 7-round initialization phase
  - Most attacks either violate security claims or target weak key spaces
  - The only valid 7-round key recovery [1] requires 2^{123} time complexity
  - Baudrin et al. recovered the entire capacity in practical time [2] but could not transition to key recovery

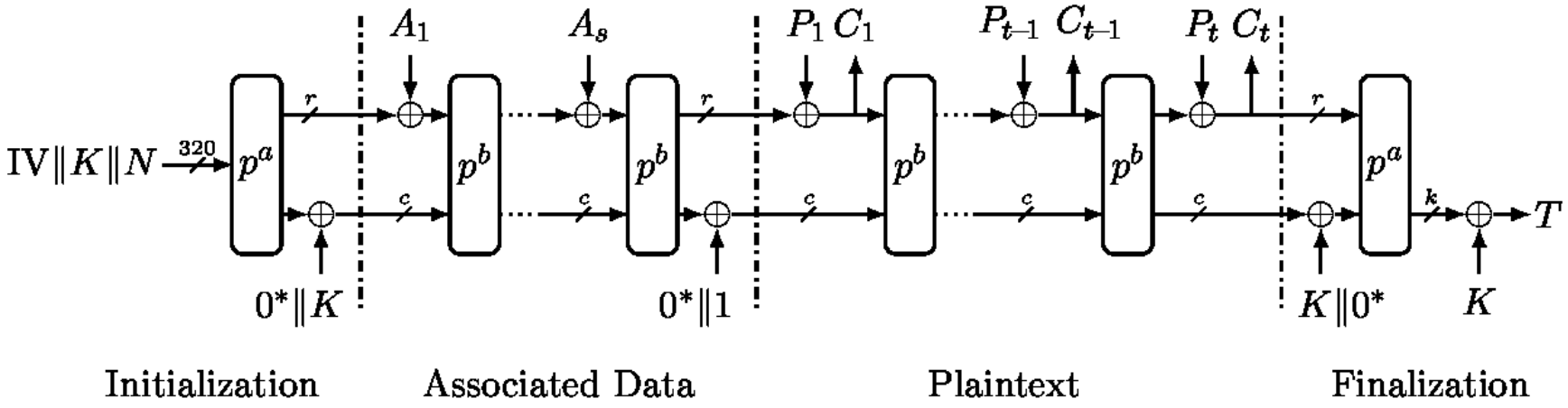
Contribution

- 7-round key recovery in the misuse-free setting with $2^{95.96}$ time complexity
- 8-round and 9-round key recovery in the misused setting
- Answer the question of how to transition the capacity recovery to key recovery

RSAC™ 2025 Conference

The Ascon AEAD

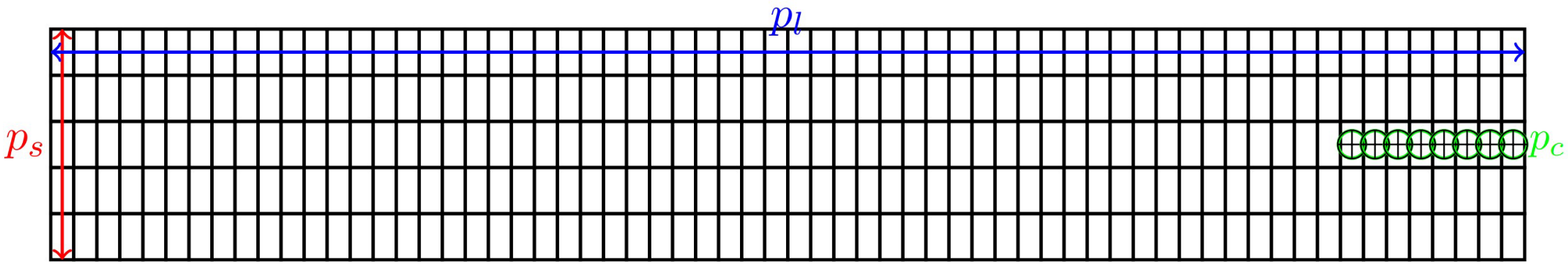
The Ascon AEAD



Name	State size	Rate r	Size of			Rounds		IV
			Key	Nonce	Tag	p^a	p^b	
Ascon-128	320	64	128	128	128	12	6	80400c0600000000
Ascon-128a	320	128	128	128	128	12	8	80800c0800000000
Ascon-80pq	320	64	160	128	128	12	6	a0400c06

In our attack, we primarily focus on the initialization phase of ascon-128

One-round permutation p



- Addition of constants (p_c): XORing an 8 bit constant to the third row
- Substitution layer (P_s): 64 parallel calls to a S-box on each column
- Linear diffusion layer (p_l): Five different linear functions applied to each row

$$p_l: \quad X_i \leftarrow \sum_i(Y_i) = Y_i + (Y_i >>> a_i) + (Y_i >>> b_i)$$

Properties of Ascon

S-box

$$
\begin{aligned}
Y_0[j] &= X_4[j]X_1[j] + X_3[j] + X_2[j]X_1[j] + X_2[j] + X_1[j]X_0[j] + X_1[j] + X_0[j] \\
Y_1[j] &= X_4[j] + X_3[j]X_2[j] + X_3[j]X_1[j] + X_3[j] + X_2[j]X_1[j] + X_2[j] + X_1[j] + X_0[j] \\
Y_2[j] &= X_4[j]X_3[j] + X_4[j] + X_2[j] + X_1[j] + 1 \\
Y_3[j] &= X_4[j]X_0[j] + X_4[j] + X_3[j]X_0[j] + X_3[j] + X_2[j] + X_1[j] + X_0[j] \\
Y_4[j] &= X_4[j]X_1[j] + X_4[j] + X_3[j] + X_1[j]X_0[j] + X_1[j]
\end{aligned}
$$

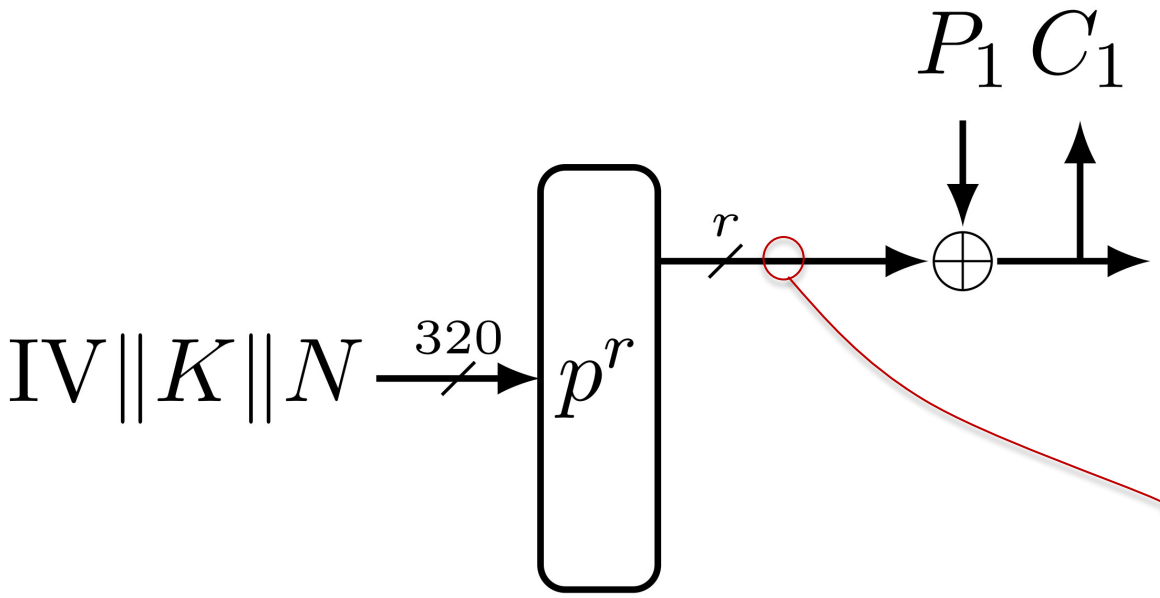
- The last row never multiplies with the third row
- For $r \in \{0, \ldots, 7\}$, the degree of the state is at most 2^r
- If one row of nonce are constants, the degree of *the state* is at most 2^{r-1}
- Conditional cube: when the nonces of two rows are equal, the degree of the state will decrease
- Borderline cube: When only the last row contains public variables, the superpoly never depends on the third row

RSAC 2025 Conference

Key recovery in the misuse-free setting

Attack mode

Target the 7-round initialization phase



- the nonce respective setting
- the data complexity does not exceed 2^{64}

- Recover the superpoly of the rate in the 6.5-round
- The rate value in the 6.5-round can be deduced by the 7-round rate
- Make several calls to the 7-round initialization process to obtain the value of the superpoly

Choose cube

- Using the borderline cube, the last row is chosen as cube variables, making the superpoly depend only on the third-row 64-bit key

1	0	0	0	0	0	0	0	0	1	0	0	…	0	0	0	0	0	0	0	0	0	0	0	0
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	…	k_{51}	k_{52}	k_{53}	k_{54}	k_{55}	k_{56}	k_{57}	k_{58}	k_{59}	k_{60}	k_{61}	k_{62}	k_{63}
k_{64}	k_{65}	k_{66}	k_{67}	k_{68}	k_{69}	k_{70}	k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	…	k_{115}	k_{116}	k_{117}	k_{118}	k_{119}	k_{120}	k_{121}	k_{122}	k_{123}	k_{124}	k_{125}	k_{126}	k_{127}
0	0	0	0	0	0	0	0	0	0	0	0	…	0	0	0	0	0	0	0	0	0	0	0	0	0
x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	…	x_{51}	x_{52}	x_{53}	x_{54}	x_{55}	x_{56}	x_{57}	x_{58}	x_{59}	x_{60}	x_{61}	x_{62}	x_{63}

Superpoly recovery(offline phase)

- Back extension to 5-round state

E.g. the first bit

$$Y_0^6[0] \rightarrow \begin{cases} X^5[153] \cdot X^5[217] \cdot X^5[255] \cdot X^5[319] \\ X^5[64] \cdot X^5[87] \cdot X^5[192] \cdot X^5[279] \\ X^5[45] \cdot X^5[67] \cdot X^5[109] \cdot X^5[195] \\ \cdots \cdots \end{cases}$$

Two MILP model: 1-4 round model and 5-6.5 round model

Using three-subset bit-based division property without unknown[3] and MILP solvers (Gurobi), we identify 121 monomials that contribute to the superpoly

Superpoly recovery(offline phase)

- Recover all degree-16 monomials and their coefficients for the 5-round state
- Compute the superpoly using the 121 monomials

$$E.g.\ X^5[153] \cdot X^5[217] \cdot X^5[255] \cdot\ X^5[319]$$

- Only products of degree-16 monomials in $X^5[153]$, $X^5[217]$, $X^5[255]$ and $X^5[319]$ can contribute to the superpoly
- Suppose $P_{153}(k)$, $P_{217}(k)$, $P_{255}(k)$ and $P_{319}(k)$ be the coefficient of degree-16 monomial which can contribute to the superpoly
- We store the product form as follows:

$$P_{153}(k) \cdot P_{217}(k) \cdot P_{255}(k) \cdot P_{319}(k)$$

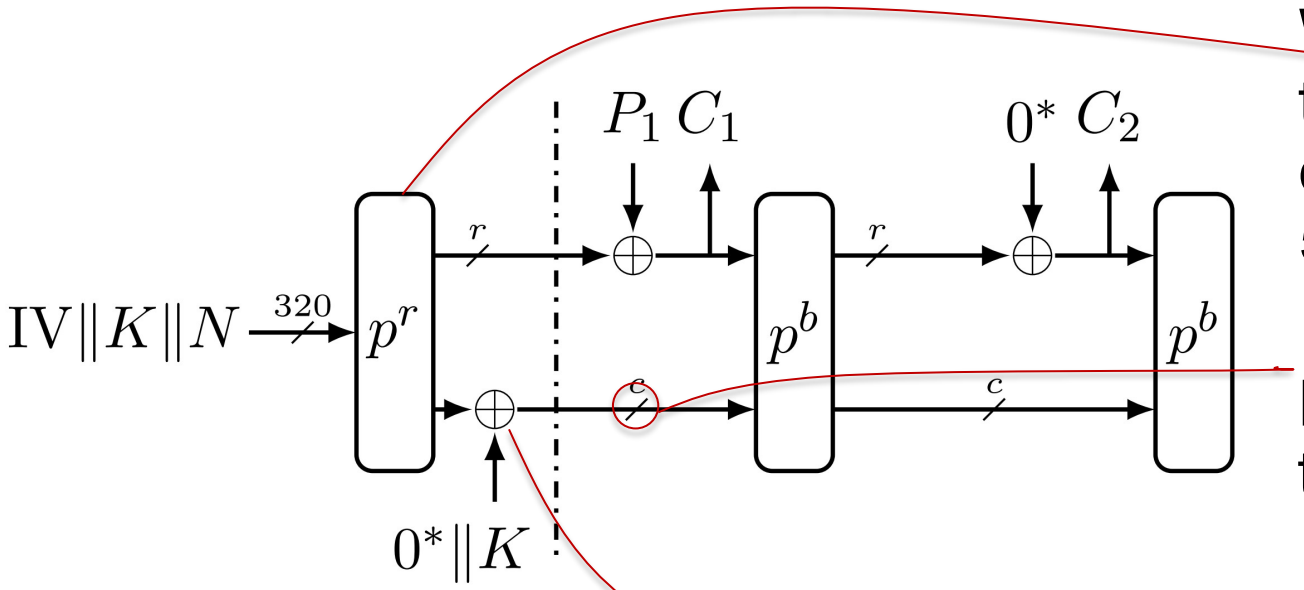
Key recovery

- The values of 64 superpolys can be obtained by 2^{64} calls of 7-rounds initialization
- Only 64 bit key are involved in the ANF of superpoly
- Suppose all 64 superpolys are balanced Boolean functions, only one key is suggested
- Exhaustive search for the remaining 64-bit key
- Complexity
  - Time: $2^{95.96}$(mainly the superpoly recovery)
  - Data: 2^{64}
  - Memory: $2^{104.85}$

RSAC 2025 Conference

Key recovery in the misused setting

Attack mode



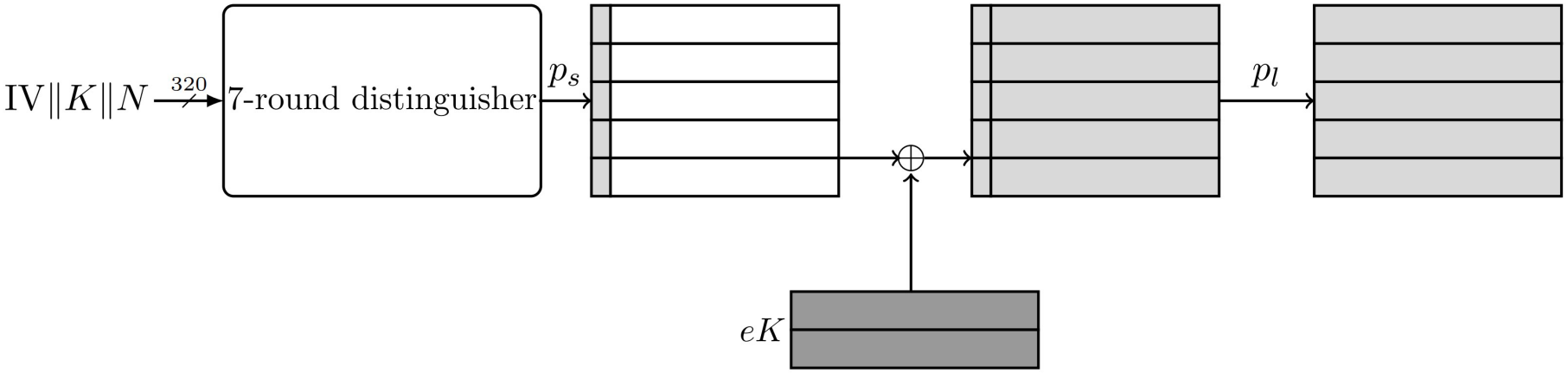
With a 61-dimension conditional cube, the superpoly will equal 0, forming a distinguisher(the 7-round degrees are 59, 59, 60, 60, and 58) [2]

Recover all states via Baudrin et al.'s technique [1]

Since the key is XORed to the state, decrypting the capacity reveals the key

- The nonce will be reused
- The date complexity will exceed 2^{64}

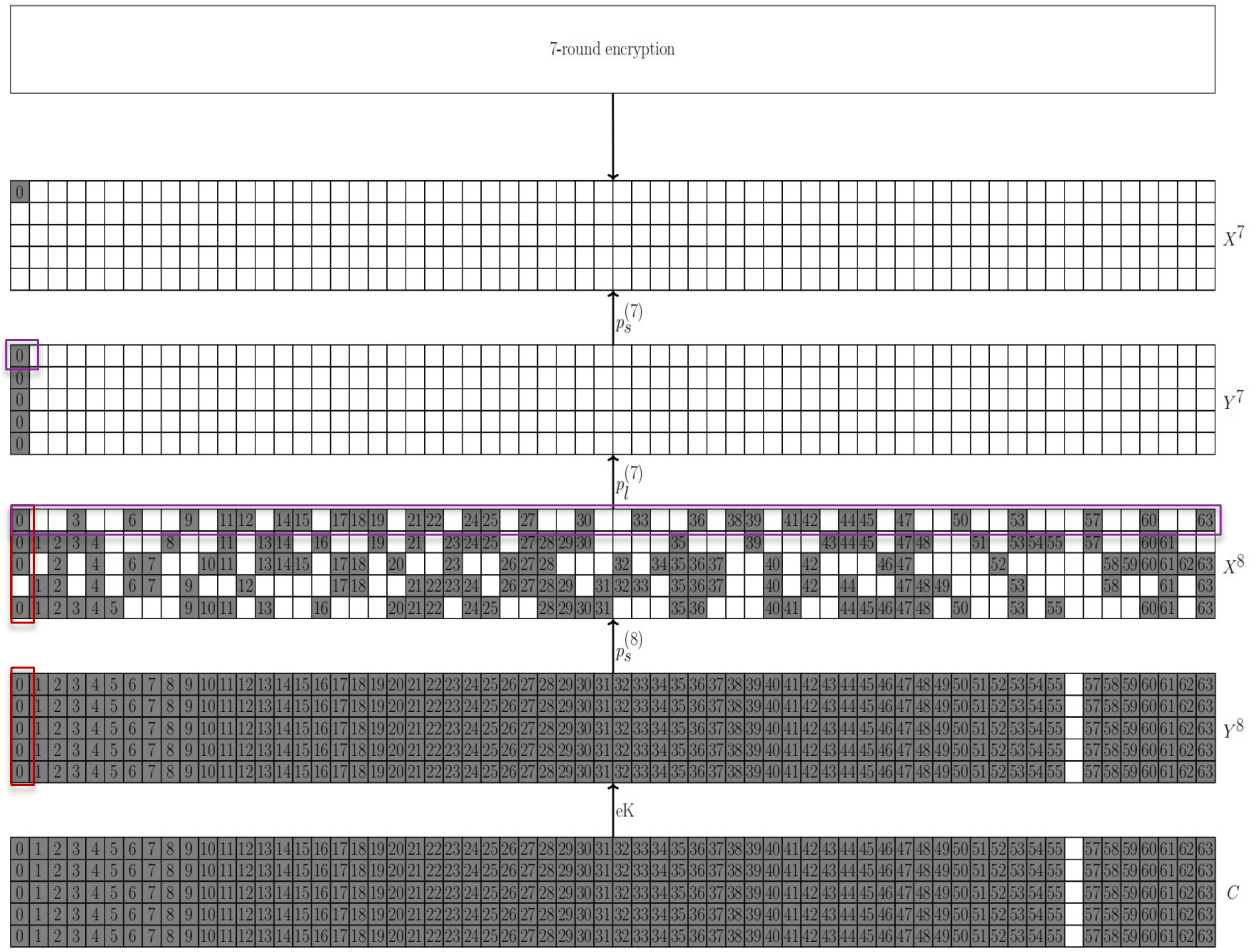
8-round key recovery



- Recover all states before encryption for 2^{61} nonces under the same key
- Extend one round after the distinguisher and decrypt backward
- Reordering is valid as p_l and key XOR are linear.
- Complexity: time 2^{101}, data 2^{101} , memory $2^{69.32}$

9-round key recovery

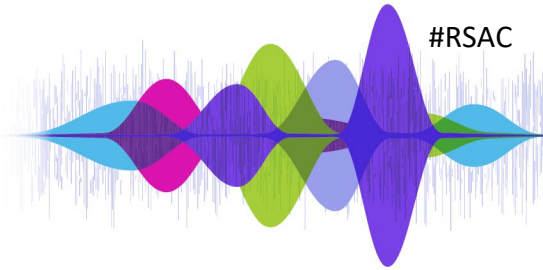
- Extend the distinguisher by two rounds for 9-round initialization
- 63 columns are involved
- S-boxes are applied separately
- The Output of $M_i \times X_i^r$ is a linear combination X_i^r
- Secret key can be guessed sequentially, lowering the complexity
- The partial-sum technique[4], introduced by Ferguson et al., reduces the key recovery complexity



山东大学 SHANDONG UNIVERSITY
RSAC 2025 Conference

9-round key recovery

- Guess key strategy
  - Using partial-sum, guess the 2-bit key, decrypt through p_s^8 and p_l^7, and calculate the contribution to $Y_i^7[0]$
  - The maximum complexity to guess the last column's key is $2^{127.92}$ Sbox computation
  - Decrypt $Y_i^7[0]$ to $X_i^7[0]$, with 2^{126} guessed keys cost 2^{132} Sbox computation
  - Exhaustive search the remaining 2^{123} key space
- Complexity
  - Time: $2^{132}/(64 \times 9) + 2^{123} \approx 2^{123.92}$
  - Data: 2^{101}
  - Memory: $2^{69.32}$



Conclusion

- Decrease the time complexity for 7-round key recovery for Ascon-128 in the misuse-free setting
- Present the 8-round and 9-round key recovery for Ascon-128 in the misused setting
- The 7-round key recovery is also appliable for Ascon-128a with the same result
- If the capacity is recovered, our attack in the misused setting is also useful in other AEAD mode

RSAC™ 2025 Conference

Many Voices.
One Community.

Thanks for your attention!

Reference

- Baudrin, J., Canteaut, A., Perrin, L.: Practical cube attack against nonce misused ascon. IACR Trans. Symmetric Cryptol. **2022**(4), 120–144 (2022). https://doi.org/10.46586/TOSC.V2022.I4.120-144, https://doi.org/10.46586/tosc.v2022.i4.120-144
- Rohit, R., Hu, K., Sarkar, S., Sun, S.: Misuse-free key-recovery and distinguishing attacks on 7-round ascon. IACR Trans. Symmetric Cryptol. **2021**(1), 130–155 (2021). https://doi.org/10.46586

- Hao, Y., Leander, G., Meier, W., Todo, Y., Wang, Q.: Modeling for three-subset division property without unknown subset - improved cube attacks against trivium and grain-128aead. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12105, pp. 466–495. Springer (2020). https://doi.org/10.1007/978-3-030-45721-1_17, https://doi.org/10.1007/978-3-030-45721-1_17

- Ferguson, N., Kelsey, J., Lucks, S., Schneier, B., Stay, M., Wagner, D.A., Whiting, D.: **Improved Cryptanalysis of Rijndael.** In: Schneier, B. (ed.) *Fast Software Encryption, 7th International Workshop (FSE 2000),* New York, NY, USA, April 10–12, 2000, Proceedings. *Lecture Notes in Computer Science,* vol. 1978, pp. 213–230. Springer (2000). https://doi.org/10.1007/3-540-44706-7_15